Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

26 643 Informatie- en communicatietechnologie (ICT)

Nr. 341 BRIEF VAN DE MINISTER VAN VEILIGHEID EN JUSTITIE

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 18 december 2014

Hierbij bied ik uw Kamer, vanuit mijn coördinerende verantwoordelijkheid voor cybersecurity, de eerste voortgangsbrief over de implementatie van het werkprogramma bij de tweede Nationale Cyber Security Strategie (NCSS 2) aan.[1]

Het werkprogramma van de NCSS 2 loopt tot en met 2016 en bouwt voort op het fundament dat in de eerste Nationale Cyber Security Strategie is gelegd. De NCSS 2 geeft het strategische kader weer waarbinnen de Nederlandse cyber security-activiteiten worden vormgegeven. Dit gebeurt interdepartementaal en publiek-privaat. De inzet van de NCSS 2 is Nederland internationaal leidend te maken op het gebied van cybersecurity.

De NCSS 2 en de activiteiten die daarbinnen plaatsvinden vormen dan ook de basis voor de Nederlandse inbreng in, en werken toe naar, de Global Conference on Cyber Space 2015 (GCCS 2015) in Den Haag en het Nederlandse EU voorzitterschap in 2016. Op 16 en 17 april 2015 is Nederland gastheer van de GCCS 2015, een internationale top met nationale vertegenwoordigers op ministerieel niveau, internationale organisaties en leiders uit de particuliere sector. De GCCS 2015 versterkt de Nederlandse positie in de internationale samenwerking op het domein van cybersecurity en cyberspace, zodat dreigingen internationaal kunnen worden aangepakt en de kansen van het internet optimaal worden benut. De GCCS 2015 in Den Haag is de vierde in een reeks van cyberspace conferenties na Londen 2011, Boedapest 2012 en Seoel 2013. Met de GCCS 2015 werkt Nederland actief mee aan een open, vrij en veilig internet. Tijdens het Nederlandse EU voorzitterschap zal cybersecurity ook één van de speerpunten zijn waarbij de nadruk onder andere wordt gelegd op nauwere Europese samenwerking, de bestrijding van cybercrime en publiek-private samenwerking.

[1] Kamerstuk 26 643, nr. 291

kst-26643-341
ISSN 0921 - 7371
's-Gravenhage 2014

Sinds het verschijnen van de NCSS 2 in 2013 is de internationale veiligheidsomgeving voor Nederland veranderd. In de, op 14 november door de Minister van Buitenlandse Zaken aan uw Kamer gezonden beleidsbrief: «Internationale veiligheid – turbulente tijden in een instabiele omgeving»,[2] geschetste ontwikkelingen raken ook het cyberdomein. De consequenties van deze ontwikkelingen worden bezien en meegenomen in de verdere ontwikkeling van de Nederlandse cybersecurity aanpak.

Om invulling te geven aan de ambities in de NCSS 2 zijn vijf doelstellingen geformuleerd:

1. Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein;
2. Nederland pakt cybercriminaliteit aan;
3. Nederland investeert in veilige en privacybeschermende ICT-producten en -diensten;
4. Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein; en
5. Nederland beschikt over voldoende cybersecuritykennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen.

Om deze doelstellingen te halen zijn in het werkprogramma 10 speerpunten en 37 actiepunten geformuleerd die door middel van publiek-private samenwerking worden gerealiseerd. 2014 was het eerste volle jaar van uitvoering van de nieuwe strategie. De resultaten treft u hieronder aan, in het besef dat de uitvoering in volle gang is en in 2015 en 2016 verder vorm krijgt. De publiek-private Cyber Security Raad monitort de uitvoering van de NCSS-2 nauwgezet. De CSR heeft zijn waardering uitgesproken voor de ingezette lijn, maar stelt tegelijkertijd dat een constante inzet noodzakelijk blijft.

Hieronder informeer ik uw Kamer, aan de hand van de 10 speerpunten, over de voortgang van het werkprogramma van de NCSS 2. In de bijlage bij deze brief is het volledige overzicht van de voortgang op alle 37 actielijnen opgenomen.

Voortgang NCSS2

Aanpak vitaal: risicoanalyses, veiligheidseisen en informatiedeling

Vitale infrastructuur is cruciaal voor het goed functioneren van onze samenleving. Onder vitale infrastructuur verstaan we producten, diensten en de onderliggende processen die, als zij uitvallen, maatschappelijke ontwrichting kunnen veroorzaken. Het is daarom belangrijk om deze vitale processen en objecten te beschermen tegen uitval door storingen, rampen, sabotage of aanslagen. Om het beschermingsniveau van de vitale sectoren in Nederland hoog te houden, werken overheid en bedrijfsleven samen aan het verder verbeteren van continuïteit en security door meer focus en samenhang aan te brengen. Daarom heeft in het afgelopen jaar een «herijking» van de vitale sectoren plaatsgevonden. Doel van deze herijking is om een actuele lijst van vitale diensten en processen te definiëren, die een goede basis vormt voor samenhang en prioriteitsstelling van verdere verhoging van de weerbaarheid van vitale sectoren. Belangrijk is dat beschermingsmaatregelen van individuele bedrijven of organisaties die onderdeel vormen van een vitale infrastructuur, goed in verhouding staan tot de risico's die soms sector overstijgend kunnen zijn. De samenhang tussen fysieke security en cybersecurity is daarbij een bijzonder aandachtspunt. Het resultaat van dit

[2] Kamerstuk 33 694, nr. 6

traject wordt momenteel afgestemd met relevante partijen. Aan de resultaten van deze inventarisatie is een programma gekoppeld voor het opstellen van roadmaps waarin, op basis van risicoanalyses maatregelen in kaart worden gebracht. Hiermee bieden de roadmaps een uitgangspunt voor weerbaarheid verhogende afspraken en maatregelen. De roadmaps zullen in de komende periode door de sectoren en vakdepartementen verder worden ingevuld. Ook is cybersecurity geïntegreerd in de systematiek van het Alerteringssysteem Terrorismebestrijding.

De Nationale Academie voor Crisisbeheersing heeft cybersecurity in de basis- en verdiepingstraining opgenomen, waarbinnen een trainingsprogramma voor respons op grootschalige ICT-incidenten is opgenomen. Binnen vitale sectoren vinden regelmatig oefeningen plaats, zowel voor afzonderlijke als samenwerkende bedrijven. In 2015 vindt een publiek-private ICT-crisisoefening op nationaal niveau plaats, waarvan de voorbereiding zijn gestart. Internationaal gezien hebben de Nucleair Security Summit (februari 2014) en de internationale oefening @tomic2014 (februari 2014) plaatsgevonden.

Zowel publieke als private partijen vervullen bij de aanpak vitaal een cruciale rol en worden nauw betrokken. Ook vanuit private partijen wordt initiatief genomen. TenneT en Shell hebben een samenwerking geïnitieerd om kwetsbaarheden, afhankelijkheden en maatregelen in de energievoorzieningsketen in kaart te brengen.

Gedragen standaarden en security en privacy by design

Veel oudere ICT systemen die thans in gebruik zijn, waren nog niet ontwikkeld met privacy en veiligheid in gedachte. Om op de lange termijn over veiligere ICT-systemen te kunnen beschikken, zet het kabinet in op het stimuleren van de ontwikkeling en aanschaf van veilige hard- en software. In 2014 is een overzicht gemaakt van relevante standaarden, waarin onderscheid is gemaakt naar doel, doelgroep en mate van toepassing die gebruikt kunnen worden voor het vergroten van de digitale veiligheid van vitale processen. Er is een publiek privaat platform internetstandaarden ingericht dat deze problematiek verder oppakt. Hierin zullen zowel de betrokken partijen die standaarden ontwikkelen als de partijen die deze moeten implementeren gaan plaatsnemen. Dit platform is in september 2014 van start is gegaan.

Met het oog op het versterken van de digitale veiligheid van ICT systemen van de rijksoverheid is in 2014 een handreiking gemaakt voor het opnemen van security eisen bij aanbestedingen. In 2013 is «het toetsmodel Privacy Impact Assessment» (PIA) voor de Rijksdienst gepubliceerd dat bij de ontwikkeling van nieuwe wetgeving en beleid en de hiermee verbonden bouw van nieuwe ICT-systemen of de aanleg van grote databestanden gebruikt kan worden. In het Rijksbrede handboek «grote projecten» is opgenomen dat beveiligingseisen onderdeel moeten zijn van de aanbesteding en dat het verplicht is een PIA uit te voeren. Nederland ICT heeft in samenwerking met de Taskforce Bestuur, Informatieveiligheid en Dienstverlening, ingesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties[3], begin november 2014 een handreiking uitgebracht voor goed opdrachtgeverschap informatieveiligheid. Het Centrum Informatiebeveiliging en privacybescherming (CIP) heeft een handreiking opgeleverd: «Grip op beveiliging in inkoopcontracten».

[3] Kamerstuk 26 643, nr. 275

Haalbaarheidsonderzoek gescheiden netwerk vitaal

In publiek-privaat verband is in 2014 een verkenning uitgevoerd naar een gescheiden ICT-netwerk voor (publieke en private) vitale processen. De verkenning geeft enerzijds inzicht in het feit dat een volledig gescheiden netwerk of het gesloten maken van delen van het internet op zichzelf geen realistische opties zijn. Het open karakter is de intrinsieke waarde die het internet vertegenwoordigt. Anderzijds wordt geconcludeerd dat de onderliggende belangen beschikbaarheid, integriteit en vertrouwelijkheid blijvend beschermd dienen te worden. Dit kan betekenen dat op basis van een uitvoerige risicoanalyse door eigenaren van informatiesystemen wordt besloten tot het creëren van een veilige omgeving middels bij de situatie passende (scheidings-) maatregelen, zoals o.a. ook plaatsvindt binnen de rijksoverheid door fysieke en/of virtuele scheiding van specifieke netwerkvoorzieningen. Voor een nadere toelichting op de bevindingen van dit haalbaarheidsonderzoek verwijs ik uw Kamer naar mijn brief van 24 november 2014[4] waarin ik uw Kamer over de bevindingen van deze verkenning heb geïnformeerd.

Versterkte aanpak cyberspionage

Cyberspionage is één van de twee grootste dreigingen waarmee Nederland op dit moment op het gebied van cyber security wordt geconfronteerd. Het aantal digitale spionageaanvallen is toegenomen, evenals de complexiteit en de impact van deze aanvallen. Bijna elke buitenlandse inlichtingendienst heeft de afgelopen jaren geïnvesteerd in zijn digitale capaciteiten. Mede vanwege de toegenomen complexiteit en impact van cyberaanvallen is stevig geïnvesteerd in de versterking van de onderzoeks- en analysecapaciteiten van de Algemene Inlichtingen en Veiligheidsdienst (AIVD), Militaire Inlichtingen en Veiligheidsdienst (MIVD) en het Nationaal Cyber Security Centrum (NCSC). In dit kader is in 2014 de oprichting van de Joint Sigint Cyber Unit (JSCU) van de AIVD en MIVD gerealiseerd en zijn de onderzoeks- en analysecapaciteiten van de AIVD en de MIVD versterkt. Het betreft hier onder andere de personele en organisatorische versterking van deze organisaties. Ook wordt verkend hoe de samenwerking tussen deze partijen kan worden versterkt op het gebied van informatiedeling over digitale aanvallen en gezamenlijke analyses, binnen de geldende juridische kaders.

Versterking Nationaal Cyber Security Centrum (NCSC)

Om adequaat invulling te geven aan zijn taken is het NCSC in personele zin in 2014 versterkt. Hiermee is de bestaande waakdienst van het NCSC verbreed tot een Nationaal Cyber Security Operations Center (NCSOC), dat 24 uur per dag, 7 dagen in de week beschikbaar is als meldpunt, nieuwe dreigingen signaleert en haar netwerk van contacten van opvolgbare informatie voorziet. Het NCSOC moet, met hulp van het Nationaal Detectie Netwerk (NDN), gaan zorgdragen voor het situationeel beeld ten aanzien van cyberdreigingen. Het NDN is een samenwerkingsverband, waarbinnen NCSC, AIVD en MIVD gezamenlijk met andere overheids- en marktpartijen optrekken, om de vroegtijdige detectie van cyberdreigingen te faciliteren. In 2014 is het basisnetwerk ontwikkeld en gerealiseerd dat in 2015 en verder uitgebouwd zal worden. Momenteel bevindt het NDN zich in de pilotfase voor rijksoverheid en is de samenwerking van start gegaan door informatiedeling met private partijen in vitale sectoren. De werking van het NDN is aanvullend op de eigen detectie-inspanningen van de organisaties. Het NDN sluit aan op het eveneens publiek-private Nationaal Respons Netwerk (NRN) dat, onder de

[4] Kamerstuk 26 643, nr. 337

coördinatie van het NCSC, de gezamenlijke respons op cybersecurity-incidenten versterkt. Het NRN is op 17 april 2014 met vijf organisaties gelanceerd en wordt momenteel verder uitgebouwd.

Internationale aanpak cybercriminaliteit: actualisatie en versterking (straf)wetgeving

In het CSBN-4 wordt geconstateerd dat cybercrime de andere grote dreiging op het gebied van cybersecurity is, naast aanvallen door statelijke actoren. Om de aanpak van cybercrime stevig aan te pakken wordt de (straf)wetgeving versterkt. Hiertoe is het wetgevingstraject voor de wet computercriminaliteit III ingezet. De wet computercriminaliteit III geeft de Nationale Politie meer slagkracht op het gebied van o.a. cybercrime. Het wetsvoorstel wordt in de eerste helft van 2015, enige tijd later dan eerder was voorzien, aan de Kamer gezonden. Internationaal wordt ingezet op het versterken van de samenwerking en het harmoniseren van wetgeving. Daarom staat het thema cybercrime op de agenda tijdens de Global Conference on Cyberspace 2015 en het Nederlandse EU voorzitterschap in 2016. Op operationeel niveau heeft de politie een personele versterking van onderzoeks- en analyse-capaciteiten doorlopen door uitbreiding van het Team High Tech Crime (THTC) van de Nationale Politie conform eerdere afspraken. Daarnaast is er internationaal een intensieve samenwerking tot stand gekomen tussen het THTC, EC3 (Europol) en IGCI (INTERPOL).

Cyberdiplomatie: kennisknooppunt voor Conflictpreventie

Met de Global Conference on Cyberspace 2015 levert Nederland een bijdrage aan de vormgeving van gedragen normen voor verantwoordelijk gedrag en de toepassing van internationaal recht in cyberspace. Ook vertrouwenwekkende maatregelen worden besproken, die een bijdrage kunnen leveren aan het vergroten van de internationale stabiliteit en aan het voorkomen van escalatie van cyberconflicten. Hierbij kan gedacht worden aan het versterken van de samenwerking tussen Computer Emergency Respons Team's (CERT's), het delen van informatie over de aanpak van cyberincidenten, nationale cyber strategieën en contactpunten. In dat kader speelt Nederland een rol in het verder vormgeven en implementeren van zulke *confidence building measures* in de OVSE. Bij het Ministerie van Buitenlandse Zaken zal na de Global Conference on Cyberspace 2015 een Task Force Cyber vorm blijven geven aan cyberdiplomatie. Nederland zet daarnaast in op het duurzaam stimuleren van cybercapaciteitsopbouw in internationaal verband, zowel in minder cyber-ontwikkelde landen als in landen waar het cyberdomein relatief ver ontwikkeld is. Het gaat daarbij om het delen van kennis en expertise op een aantal centrale cyberthema's tussen internationale publieke en private partners.

Versterking civiel-militaire samenwerking

Militaire en civiele actoren zijn in het digitale domein steeds meer met elkaar verweven. Een civiel-militaire aanpak ter vergroting van de digitale veiligheid is daarom noodzakelijk. In 2014 zijn forse stappen gezet in de opbouw van Defensie cybercapaciteiten. Met de lancering van het Defensie Cyber Commando in oktober jl. is de eerste stap gezet richting een operationele cybercapaciteit. In 2014 is tevens het Defensie Cyber Expertise Centrum (DCEC) opgericht voor kennisontwikkeling, opleiding van het personeel, innovatie en onderzoek. Er wordt geïnvesteerd in de verdere ontwikkeling van het inlichtingenvermogen en operationele cybercapaciteit en er wordt een doctrine opgesteld voor de inzet van cybercapaciteiten in militaire operaties. In 2015 wordt de Defensie Cyber

Strategie geactualiseerd, die de komende jaren richting geeft aan de doorontwikkeling van cybercapaciteiten bij Defensie. Met het oog op de beschikbaarheid van voldoende gekwalificeerd personeel in het geval van cyberincidenten is in 2014 een Defensie cyberreservistenbestand opgericht. Dit bestand zal in de komende jaren verder worden gevuld.

Tussen het Ministerie van Veiligheid en Justitie en het Ministerie van Defensie is regulier en nauw contact over de ontwikkeling van cybercapaciteiten en het vormgeven van de civiel-militaire samenwerking. Per op te bouwen Defensiecapaciteit wordt bezien of en hoe deze ter ondersteuning van civiele partijen kan worden ingezet. Om de samenwerking te faciliteren zijn in 2014 wederzijdse detacheringen van functionarissen van de NCSC en het Defensie Cyber Commando overeengekomen. Daarnaast heeft de samenwerking tussen DefCERT en het NCSC een permanente en formele status gekregen met het ondertekenen van een samenwerkingsconvenant.

Cybersecurity onderwijs

Om de behoefte aan cybersecurity onderwijs in Nederland inzichtelijk te maken en een impuls te geven zal langs verschillende wegen onderzoek worden gedaan en onder regie van VenJ en OCW het gesprek tussen de betrokken partijen worden georganiseerd. Een aantal HBO-lectoren heeft medewerking toegezegd aan de ontwikkeling van een onderwijsagenda voor het HBO. Hierbij wordt de samenwerking gezocht met het (door OCW gefinancierde) Regieorgaan SIA en het Cybersafety Research and Education Network. Voor het MBO wordt aansluiting gezocht bij lopende initiatieven rond informaticaonderwijs en het Techniekpact.
Ook is in 2014 de Cyber Security Academie opgericht, die een post-doctorale masteropleiding cybersecurity verzorg en die recent is gestart met 20 studenten. Het WODC heeft een onderzoek uitgezet naar de vraag naar diverse soorten werknemers die een rol spelen bij cybersecurity en het aanbod aan onderwijs waarlangs deze worden opgeleid en om/bijgeschoold. Dit onderzoek wordt begin 2015 opgeleverd.

Stimuleren van innovatie in cybersecurity

Om innovatie in cybersecurity te stimuleren krijgt onderzoek een impuls en worden stappen gezet om een verbeterd inzicht te krijgen in de onderzoek behoefte van bedrijfsleven en maatschappij en het realiseren van een betere aansluiting tussen wetenschap en praktijk. Agentschap NL/RvO en NWO hebben, binnen de kaders van de in 2012 gelanceerde Nationale Cyber Security Research Agenda II (NCSRA II), een tweede tender voor de NCSRA in juni 2014 uitgeschreven ter waarde van ongeveer € 5,5 miljoen, ongeveer gelijk verdeeld over een SBIR programma voor korte termijn R&D en lange termijn onderzoek.

Tot slot

De realisatie van het werkprogramma van de NCSS 2 is door betrokken publieke en private partijen actief ter hand genomen. Hiermee worden belangrijke stappen gezet om de weerbaarheid van Nederland te versterken en vinden investeringen plaats om bij te blijven bij de snelle ontwikkelingen op het cyberdomein. Het Cyber Security Beeld Nederland (CSBN), dat een belangrijk uitgangspunt vormt voor het de NCSS 2 laat zien dat de in het CSBN 2013 geconstateerde trends en ontwikkelingen zich doorzetten in 2014.[5] Dit bevestigt het belang van de met de NCSS 2 ingeslagen weg. Het kabinet investeert daarom ook de komende jaren, in

[5] Kamerstuk 26 643, nr. 285

publiek-private participatie, samen met kennisinstellingen en vitale sectoren, onverminderd in cybersecurity. De ontwikkelingen in het cyberdomein zullen daarbij nauwlettend worden gevolgd zodat, wanneer dat nodig is naar aanleiding van technische of maatschappelijke ontwikkelingen, acties aangescherpt of geïntensiveerd worden en actief kan worden ingespeeld op ontwikkelingen.

De Minister van Veiligheid en Justitie,
I.W. Opstelten

Bijlage:

Stand van zaken werkprogramma NCSS-2

Doelstelling 1: Nederland is weerbaar tegen cyberaanvallen en beschermt zijn vitale belangen in het cyberdomein (actiepunten 1 tot en met 15)

Doelstelling 1 van de NCCS-2 richt zich op het versterken van de weerbaarheid van de Nederlandse maatschappij tegen cyberaanvallen die gericht zijn op de vitale belangen van Nederland. Zowel publieke als private partijen vervullen hierbij een cruciale rol. Zij verenigen zich als netwerken op alle niveaus en in diverse samenstellingen. Om dit mogelijk te maken is een aantal publiek-private samenwerkingsvormen in het leven geroepen op strategisch, tactisch en operationeel niveau (onder andere Information Sharing and Analysis Centres (ISAC's) en internationale Computer Emergency Respons Team's (CERT's). Ook zijn diverse private initiatieven genomen zoals een Proof of Concept dat door TenneT en Shell is geïnitieerd voor de verhoging van de weerbaarheid van de energievoorzieningsketen. Bij de versterking van de weerbaarheid wordt ingezet op operationele capaciteiten (detectiecapaciteiten, duidingscapaciteiten, alerteringsmogelijkheden, responscapaciteiten, crisisbeheersing) en het stimuleren van het gebruik van veilige ICT bij de rijksoverheid en in de vitale infrastructuur.

Aanpak vitaal (actiepunten 1 en 11)

Vitale infrastructuur is cruciaal voor het goed functioneren van onze samenleving. Onder vitale infrastructuur verstaan we producten, diensten en de onderliggende processen die, als zij uitvallen, maatschappelijke ontwrichting kunnen veroorzaken. Het is daarom belangrijk om deze vitale processen en objecten te beschermen tegen uitval door storingen, rampen, sabotage of aanslagen. Om het beschermingsniveau van de vitale sectoren in Nederland hoog te houden, werken overheid en bedrijfsleven samen aan het verder verbeteren van continuïteit en security door meer focus en samenhang aan te brengen. Daarom heeft in het afgelopen jaar een «herijking» van de vitale sectoren plaatsgevonden. Doel van deze herijking is om een actuele lijst van vitale diensten en processen te definiëren, die een goede basis vormt voor samenhang en prioriteitsstelling van verdere verhoging van de weerbaarheid van vitale sectoren. Belangrijk is dat beschermingsmaatregelen van individuele bedrijven of organisaties die onderdeel vormen van een vitale infrastructuur, goed in verhouding staan tot de risico's die soms sector overstijgend kunnen zijn. De samenhang tussen fysieke security en cybersecurity is daarbij een bijzonder aandachtspunt. Het resultaat van dit traject wordt momenteel afgestemd met relevante partijen. Aan de resultaten van deze inventarisatie is een programma gekoppeld voor het opstellen van roadmaps waarin, op basis van risicoanalyses maatregelen in kaart worden gebracht. Hiermee bieden de roadmaps een uitgangspunt voor weerbaarheid verhogende afspraken en maatregelen. De roadmaps zullen in de komende periode door de sectoren en vakdepartementen verder worden ingevuld. Aanpalend aan de aanpak vitaal wordt ook de problematiek van legacysytemen in kaart gebracht. Ook is cybersecurity geïntegreerd in de systematiek van het Alerteringssysteem Terrorismebestrijding.

De Nationale Academie voor Crisisbeheersing heeft cybersecurity in de basis- en verdiepingstraining opgenomen, waarbinnen een trainingsprogramma voor respons op grootschalige ICT-incidenten is opgenomen. Binnen vitale sectoren vinden regelmatig oefeningen plaats, zowel voor afzonderlijke als samenwerkende bedrijven. In 2015 vindt een publiek-private ICT-crisisoefening op nationaal niveau plaats, waarvan de

voorbereiding zijn gestart. Internationaal gezien hebben de NSS (februari 2014) en de internationale oefening @tomic2014 (februari 2014) plaatsgevonden.

Zowel publieke als private partijen vervullen bij de aanpak vitaal een cruciale rol en worden nauw betrokken. Ook vanuit private partijen wordt initiatief genomen. TenneT en Shell hebben een samenwerking geïnitieerd om kwetsbaarheden, afhankelijkheden en maatregelen in de energievoorzieningsketen in kaart te brengen.

Gedragen standaarden en security en privacy by design (actiepunten 2 en 3)

Veel oudere ICT systemen waren nog niet ontwikkeld met privacy en veiligheid in gedachten. Om op de lange termijn over veiligere ICT systemen te kunnen beschikken, zet het kabinet in op het stimuleren van de ontwikkeling en aanschaf van veilige hard- en software. In 2014 is een overzicht gemaakt van relevante standaarden, waarin onderscheid is gemaakt naar doel, doelgroep en mate van toepassing die gebruikt kunnen worden voor het vergroten van de digitale veiligheid van vitale processen. Er is een publiek privaat platform internetstandaarden ingericht dat deze problematiek verder oppakt. Hierin zullen zowel de betrokken partijen die standaarden ontwikkelen als de partijen die deze moeten implementeren gaan plaatsnemen. Dit platform is in september 2014 van start is gegaan.

Met het oog op het versterken van de digitale veiligheid van ICT systemen van de rijksoverheid is in 2014 een handreiking gemaakt voor het opnemen van security eisen bij aanbestedingen. In 2013 is «het toetsmodel Privacy Impact Assessment» (PIA) voor de Rijksdienst gepubliceerd dat de bij ontwikkeling van nieuwe wetgeving en beleid en de hiermee verbonden bouw van nieuwe ICT-systemen of de aanleg van grote databestanden gebruikt kan worden. In het Rijksbrede handboek «grote projecten» is opgenomen dat beveiligingseisen onderdeel moeten zijn van de aanbesteding en dat het verplicht is een PIA uit te voeren. Nederland ICT heeft in samenwerking met de Taskforce Bestuur Informatieveiligheid en Dienstverlening, ingesteld door de Minister van Binnenlandse Zaken en Koninkrijksrelaties[6], begin november 2014 een handreiking uitgebracht voor goed opdrachtgeverschap informatieveiligheid. Het Centrum Informatiebeveiliging en privacybescherming (CIP) heeft een handreiking opgeleverd: «Grip op beveiliging in inkoopcontracten». Als opvolging van dit actiepunt wordt nu verder gedacht aan certificering (voor ISO 27001) van interne en externe leveranciers.

Haalbaarheidsonderzoek gescheiden netwerk vitaal (actiepunt 4)

In 2014 is in publiek-privaat verband is een verkenning uitgevoerd naar een gescheiden ICT-netwerk voor (publieke en private) vitale processen. De verkenning geeft inzicht in het feit dat een volledig gescheiden netwerk op zichzelf geen realistische optie is. Dit geldt eveneens voor het gesloten maken van delen van het internet. Dit onderschrijft het door het kabinet gehechte belang aan een open en vrij internet. Het open karakter is de intrinsieke waarde die het internet vertegenwoordigt. Dit laat onverlet dat de verkenning tevens laat zien dat het van belang is om de onderliggende belangen: beschikbaarheid, integriteit en vertrouwelijkheid blijvend te beschermen. Dit kan betekenen dat op basis van een uitvoerige risicoanalyse, in het kader waarvan kosten en baten in vergelijking met verschillende alternatieven en/of aanvullende maatregelen vergeleken

[6] Kamerstuk 26 643, nr. 275

kunnen worden, door eigenaren van informatiesystemen wordt besloten tot het creëren van een veilige omgeving middels bij de situatie passende (scheidings-)maatregelen, zoals o.a. ook plaatsvindt binnen de rijksoverheid door fysieke en/of virtuele scheiding van specifieke netwerkvoorzieningen. In mijn brief van 24 november 2014[7] heb ik uw Kamer over de bevindingen van deze verkenning geïnformeerd.

Versterken detectie-, onderzoek- en analysecapaciteiten ten behoeve van onder andere aanpak cyberspionage (actiepunt 5 en 9)

Cyberspionage is één van de twee grootste dreigingen waarmee Nederland op dit moment op het gebied van cyber security wordt geconfronteerd. Het aantal digitale spionageaanvallen is toegenomen evenals de complexiteit en de impact van deze aanvallen. Bijna elke buitenlandse inlichtingendienst heeft de afgelopen jaren geïnvesteerd in zijn digitale capaciteiten. Mede vanwege de toegenomen complexiteit en impact van cyberaanvallen is stevig geïnvesteerd in de versterking van de onderzoeks- en analysecapaciteiten van de AIVD MIVD en het NCSC. In dit kader is in 2014 de oprichting van de Joint Sigint Cyber Unit (JSCU) van de AIVD en MIVD gerealiseerd en zijn de onderzoeks- en analysecapaciteiten van de AIVD en de MIVD versterkt. Het betreft hier onder andere de personele en organisatorische versterking van deze organisaties. Ook wordt verkend hoe de samenwerking tussen deze partijen kan worden versterkt op het gebied van informatiedeling over digitale aanvallen en gezamenlijke analyses, binnen de geldende juridische kaders.

Versterking Defensie cybercapaciteiten (Actiepunten 6, 14 en 15)

De versterking van de cybercapaciteiten van Defensie vormt de militaire pijler van de NCSC 2. Defensie richt zich op de versterking van zijn digitale weerbaarheid en het inlichtingenvermogen in het digitale domein. Een andere prioriteit betreft het vermogen om cyberoperaties uit te voeren ter ondersteuning van de driehoofdtaken van de krijgsmacht. In 2014 zijn forse stappen gezet. Zo is het Defensie Cyber Expertise Centrum (DCEC) opgericht voor kennisontwikkeling, opleiding van het personeel, innovatie en onderzoek. Ook heeft de MIVD de capaciteit voor inlichtingenvergaring via het digitale domein verder versterkt, waarbij de dienst nauw samenwerkt met de AIVD in de Joint Sigint Cyber Unit. Met de lancering van het Defensie Cyber Commando in oktober jl. is de eerste stap gezet richting een operationele cybercapaciteit. Het is nu vooral van belang op deze fundamenten voort te bouwen en cybercapaciteiten verder in te bedden als integraal onderdeel van het militaire optreden. Naar verwachting zal het DCC eind 2015 operationeel zijn. In de periode 2014–2015 worden verdere maatregelen genomen om de beschikbaarheid en inzetbaarheid van kritieke defensienetwerken en systemen te garanderen. Ook wordt geïnvesteerd in verdere ontwikkeling van het inlichtingenvermogen en operationele cybercapaciteit en wordt een doctrine opgesteld voor de inzet van cybercapaciteiten in militaire operaties. In 2015 wordt de Defensie Cyber Strategie geactualiseerd. De actualisering van de strategie zal de komende jaren richting geven aan de doorontwikkeling van cybercapaciteiten bij Defensie. Defensie zal onder andere investeren in de kennis en deskundigheid van haar personeel op het gebied van cyber, in relevante opleidingen, cyberwapens, detectiesystemen, een cyberlaboratorium en in capaciteit ten behoeve van datavergaring en analyse. Met het oog op de beschikbaarheid van voldoende gekwalificeerd personeel in het geval van cyberincidenten is in 2014 een Defensie cyberreservistenbestand opgericht. Dit bestand zal in de komende jaren verder worden gevuld.

---

[7] Kamerstuk 26 643, nr. 337

Versterking cybersecurity medeoverheden (Actiepunten 7 en 8)

Om het bewustzijn over cybersecurity van medeoverheden te versterken is door de Taskforce Bestuur en Informatieveiligheid Dienstverlening in 2014 gewerkt aan het committeren van medeoverheden aan een versterkte aanpak van informatieveiligheid. Middels verschillende activiteiten en instrumenten is gewerkt aan het creëren van bewustzijn bij bestuurders en managers bij de overheid. Mede naar aanleiding hiervan is recentelijk een verklaring getekend door vertegenwoordigers van het Rijk, provincies, gemeenten, waterschappen en de Manifestgroep, waarmee wordt bekrachtigd dat informatieveiligheid ook na de beëindiging van de Taskforce Bestuur en Informatieveiligheid Dienstverlening begin 2015, blijvend aandacht krijgt. Daarnaast worden in 2015, met koepelvertegenwoordigers bij de overheid, verantwoordelijkheden benoemd en procedures afgesproken voor organisatie overstijgende incidenten in het openbaar bestuur die geen crisis zijn.

Versterking Nationaal Cyber Security Centrum (Actiepunt 10)

Om adequaat invulling te geven aan zijn taken is het NCSC op het personele vlak in 2014 versterkt door een uitbreiding. Hiermee is de bestaande waakdienst van het NCSC verbreed tot een Nationaal Cyber Security Operations Center (NCSOC), dat 24 uur per dag, 7 dagen in de week beschikbaar is als meldpunt, nieuwe dreigingen signaleert en haar netwerk van contacten van opvolgbare informatie voorziet. Het NCSOC moet, met hulp van het Nationaal Detectie Netwerk (NDN) gaan zorgdragen voor het situationeel beeld ten aanzien van cyberdreigingen. Het NDN is een samenwerkingsverband, waarbinnen NCSC, AIVD en MIVD gezamenlijk met andere overheids- en marktpartijen optrekken, om de vroegtijdige detectie van cyberdreigingen, waaronder spionage, te faciliteren. In 2014 is het basisnetwerk ontwikkeld en gerealiseerd dat in 2015 en verder uitgebouwd zal worden. Momenteel bevindt het NDN zich in de pilotfase voor rijksoverheid en is de samenwerking van start gegaan door informatiedeling met private partijen in vitale sectoren. Hierbij zijn de mogelijkheden van NDN aanvullend aan de eigen detectie-inspanningen van de organisatie Het NDN sluit aan op het eveneens publiek-private Nationaal Respons Netwerk (NRN) dat, onder de coördinatie van het NCSC, de gezamenlijke respons op cybersecurity-incidenten versterkt. Het NRN is op 17 april 2014 met vijf organisaties gelanceerd en wordt momenteel verder uitgebouwd.

In 2015 te initiëren actiepunten (Actiepunten 12 en 13)

De realisatie van een aantal actiepunten start in 2015 zodat de bevindingen van andere trajecten kunnen worden meegenomen. Zo wordt de versterking van de bestaande sectorale toezichthouders door het opnemen van cybersecurity vereisten in 2015 gestart zodat de (eerste) bevindingen uit de aanpak voor de bescherming van de vitale infrastructuur in dit traject kunnen worden meegenomen. Dit geldt ook voor de verkenning naar de mogelijkheid van accreditatie van bedrijven die als «digitale brandweer» ingeschakeld kunnen worden.

Doelstelling 2: Nederland pakt cybercriminaliteit aan (actiepunten 16 tot en met 22)

In het CSBN-4 wordt geconstateerd dat cybercrime de andere grote dreiging op het gebied van cybersecurity is, samen met aanvallen door statelijke actoren. Doelstelling 2 richt zich op het versterken van de aanpak van cybercriminaliteit zowel doormiddel van de versterking van (straf)wet-

geving als door een versterking van de opsporing en vervolging van cybercrime.

Internationale aanpak cybercriminaliteit: actualisatie en versterking (straf)wetgeving (Actiepunten 16 en 17)

Om de aanpak van cybercrime stevig aan te pakken wordt (straf)wetgeving versterkt. Hiertoe is het wetgevingstraject voor de wet computercriminaliteit III ingezet. De wet computercriminaliteit III geeft de Politie meer slagkracht op het gebied van o.a. cybercrime. Het wetsvoorstel wordt in de eerste helft van 2015, enige tijd later dan eerder was voorzien, aan de Kamer gezonden. Internationaal wordt ingezet op het versterken van de samenwerking en het harmoniseren van wetgeving. Daarom staat het thema cybercrime op de agenda tijdens de Global Conference on Cyberspace 2015. Op operationeel niveau is er sprake van een intensieve samenwerking tussen de het Team High Tech Crime (THTC) van de Nationale Politie, EC3 (Europol) en IGCI (INTERPOL).

Versterking opsporing en vervolging cybercrime (Actiepunten 18, 19, 20 en 21)

De Politie heeft een personele versterking van onderzoeks- en analysecapaciteiten doorlopen door uitbreiding van het THTC conform eerdere afspraken. In 2014 is de versterking van de opsporing en vervolging van cybercrime opgenomen in de landelijke prioriteiten van de Politie en zal het Team High Tech Crime van de Politie 20 onderzoeken doen. Ook is de aanpak van cybercrime een prioriteit in de Veiligheidsagenda 2015 – 2018. Afgesproken is dat het aantal cybercrime-onderzoeken zal worden uitgebreid naar 360 onderzoeken in 2018, uitgevoerd zowel door de landelijk eenheid als de regionale eenheden. Het aantal complexe zaken loopt op tot 50 zaken in 2018, waaronder minstens 20 zaken door het THTC. Daarnaast kreeg de samenwerking tussen het Openbaar Ministerie, de politie en de financiële sector op het gebied van cybercrime o.a. vorm in de *Electronic Crimes Task Force*.

Verbeteren procedures intake en registratie voor melding en aangifte van cybercrime. (Actiepunt 22)

De activiteiten om de doelstelling te behalen vloeien voort uit de Landelijke Prioriteiten Politie 2011–2014 om de procedures voor de intake en registratie voor melding en aangifte van cybercrime te verbeteren. Dit traject is in gang gezet. Het doel is landelijk meer zicht te krijgen op daders, zaken en aangiftes en leidt tot een update van de Handreiking intake van internet gerelateerde criminaliteit, opleidingen voor politiepersoneel en de borging en verbetering van bestaande initiatieven in de staande organisatie van de Politie.

Doelstelling 3: Nederland investeert in veilige en privacybeschermende ICT-producten en -diensten (actiepunten 23 en 24)

Veel oudere ICT-producten zijn niet gebouwd met veiligheid en privacy in gedachte. Om op de lange termijn over veiligere ICT systemen te kunnen beschikken wordt ingezet op het stimuleren van de ontwikkeling veilige hard- en software en het vergroten van de bewustwording ten aanzien van veilig internetten.

Verbeteren en of ontwikkelen van standaarden om veiligheid en privacy van ICT-producten en -diensten te bevorderen (actiepunt 23)

Er wordt ingezet op het verbeteren en of ontwikkelen van internationale standaarden die gebruikt worden om veiligheid en privacy van ICT-producten en -diensten te bevorderen. Dit gebeurt zoveel mogelijk in internationaal verband. Het betreft hier een langdurige inspanning waarvoor in de NCSS-2 de eerste aanzet en kaders worden neergezet. In 2014 is hiervoor een normenkader ontwikkeld door o.a. Security Academy en iComply in nauwe samenwerking met het Ministerie van Economische Zaken en ECP Platform voor de informatiesamenleving. Het «Normenkader Secure Software» is in mei 2014 gelanceerd en sindsdien is het met succes getest bij diverse software- ontwikkelorganisaties. Momenteel wordt met private partners gekeken naar een business case om hier een vervolg aan te geven. Ook is er in 2014 een overzicht van relevante (internationale) gremia waarbinnen over standaarden en de toepassing daarvan wordt gesproken opgesteld. Daarnaast is er een gespreksagenda opgesteld ten behoeve van internationaal overleg. Aan de hand van deze agenda zal de komende jaren in relevante gremia worden ingezet op het verbeteren van standaarden om de veiligheid en privacy van ICT-producten en -diensten te bevorderen. De adoptie van standaarden is reeds aan de orde geweest tijdens de IGF in Istanbul en zal aan de orde komen tijdens de Global Conference on Cyberspace 2.

Lanceren bewustwordingscampagnes (actiepunt 24)

Van 27 oktober tot en met 6 november jl. vond wederom met de succes de derde editie van de landelijke bewustwordingscampagne Alert Online plaats. Aan Alert Online namen ruim 140 partners deel uit publiek, privaat en wetenschap. In de campagneperiode zetten alle partners zich in om intern en extern het online veiligheidsbewustzijn te vergroten bij overheid, bedrijfsleven en consumenten. Tijdens Alert Online hebben rond de externe 80 evenementen plaats gevonden en een groot aantal interne campagnes. Privacy was een van de thema's binnen het overkoepelend thema «kennis over cyber security». Daarnaast kwamen thema's als cyber security onderwijs, onderzoek, innovaties, en de online veiligheid van jongeren aan de orde in de campagne-activiteiten. Tijdens Alert Online is ook de website veiliginternetten.nl gelanceerd. Op veiliginternetten.nl worden consumenten en het midden- en kleinbedrijf geïnformeerd over wat zij zelf kunnen doen en laten om veilig online te zijn. Veiliginternetten.nl is samenwerking tussen het Ministerie van Economische Zaken, Veiligheid en Justitie en ECP-Platform voor de informatiesamenleving. Ook volgend jaar wordt onverminderd ingezet op cyber security awareness en zal van 26 oktober tot en met 6 november 2015 weer de campagne Alert Online plaatsvinden.

Doelstelling 4: Nederland bouwt coalities voor vrijheid, veiligheid en vrede in het cyberdomein (actiepunten 25 tot en met 30)

Door het wereldwijde en grensoverschrijdende karakter van cyberspace is internationale samenwerking onontbeerlijk voor het oplossen van uitdagingen omtrent cyber security en bredere vraagstukken ten aanzien van het internet. Om daarbij de Nederlandse belangen te behartigen versterkt Nederland zijn internationale diplomatieke profiel op een aantal cybergebieden als internetvrijheid en internationale vrede en veiligheid. De voornaamste activiteit daarvoor is de organisatie van de Global Conference on Cyberspace in april 2015, waarmee ook een aantal internationale actiepunten van de NCSS 2 deels wordt uitgevoerd en het Nederlandse EU-voorzitterschap van 2016.

Voeren van cyberdiplomatie, gedragsnormen en vertrouwenwekkende maatregelen (actiepunt 25)

Met de Global Conference on Cyberspace 2015 levert Nederland een bijdrage aan de vormgeving van gedragen normen voor verantwoordelijk gedrag en de toepassing van internationaal recht in cyberspace. Ook vertrouwenwekkende maatregelen worden besproken, die een bijdrage kunnen leveren aan het vergroten van de internationale stabiliteit en aan het voorkomen van escalatie van cyberconflicten. Hierbij kan gedacht worden aan het versterken van de samenwerking tussen Computer Emergency Respons Team's (CERT), het delen van informatie over de aanpak van cyberincidenten, nationale cyber strategieën, en contactpunten. In dat kader speelt Nederland een rol in het verder vormgeven en implementeren van zulke *confidence building measures* in de OVSE. Bij het Ministerie van Buitenlandse Zaken zal na de Global Conference on Cyberspace 2015 een Task Force Cyber vorm blijven geven aan cyberdiplomatie.

High level bijeenkomsten en kennisknooppunt internationaal recht en conflictpreventie (actiepunt 26)

Het streven om high level bijeenkomsten te organiseren wordt ingevuld met de GCCS 2015. De toepassing van het internationaal recht in cyberspace en conflictpreventie worden daar uitgebreid besproken onder het thema internationale stabiliteit. Ter voorbereiding daarvan worden wereldwijd een aantal inhoudelijke bijeenkomsten georganiseerd. Ook wordt bezien of in 2015 op deze onderwerpen een kennisknooppunt kan worden vormgegeven in Nederland.

Nederland blijft internationaal het voortouw nemen op het terrein van internetvrijheid (actiepunt 27)

Nederland blijft internationaal het voortouw nemen op het terrein van internetvrijheid, onder andere met de Freedom Online Coalitie (FOC), en inzetten op een krachtige Europese aanpak van privacybescherming en fundamentele rechten en waarden vis-à-vis derde landen. Internetvrijheid zal op de GCCS 2015 aan de orde komen als een hoofdthema.

Actieve deelname in internationale cyberevenementen (actiepunt 28)

Om de Nederlandse belangen te behartigen en de eigen visie voor het voetlicht te brengen participeert de Nederlandse overheid de komende jaren versterkt in cyber-gerelateerde internationale cyberconferenties, multi-stakeholderevenementen en besluitvormende evenementen.

Nederland zet in op cybercapaciteitsopbouw in internationaal verband (actiepunt 29)

Nederland zet in op het duurzaam stimuleren van cybercapaciteitsopbouw in internationaal verband, zowel in minder cyber-ontwikkelde landen als in landen waar het cyberdomein relatief verder ontwikkeld is. Het gaat daarbij om het delen van kennis en expertise op een aantal centrale cyberthema's tussen internationale publieke en private partners

Versterking civiel-militaire samenwerking (actiepunt 30)

Militaire en civiele actoren zijn in het digitale domein steeds meer met elkaar verweven. Een civiel-militaire aanpak ter vergroting van de digitale veiligheid is daarom noodzakelijk. In het kader van de NCSS 2 worden mogelijkheden uitgewerkt voor de nationale inzet van de digitale

capaciteiten van Defensie op verzoek van civiele autoriteiten. Tussen het Ministerie van Veiligheid en Justitie en het Ministerie van Defensie is regulier en nauw contact over de ontwikkeling van cybercapaciteiten en het vormgeven van de civiel-militaire samenwerking. Per op te bouwen Defensiecapaciteit wordt bezien of en hoe deze ter ondersteuning van civiele partijen kan worden ingezet. Om de samenwerking te faciliteren zijn in 2014 wederzijdse detacheringen van functionarissen van de NCSC en het Defensie Cyber Commando overeengekomen. Daarnaast heeft de samenwerking tussen DefCERT en het NCSC een permanente en formele status gekregen middels een samenwerkingsconvenant.

Doelstelling 5: Nederland beschikt over voldoende cybersecurity-kennis en -kunde en investeert in ICT-innovatie om onze cybersecuritydoelstellingen te behalen (actiepunten 31 tot en met 37)

Onder doelstelling 5 vallen het versterken van het cyber security onderwijs en onderzoek, het creëren van meer stageplekken, het versterken van de Nederlandse kennispositie en de aansluiting van cyber security onderzoek op de behoefte van het bedrijfsleven.

Versterken cybersecurity onderwijs (Actiepunt 31, 32 en 33)

Om de behoefte aan cybersecurity onderwijs in Nederland inzichtelijk te maken en een impuls te geven zal langs verschillende wegen onderzoek worden gedaan en onder regie van VenJ en OCW het gesprek tussen de betrokken partijen worden georganiseerd. Een aantal HBO-lectoren heeft medewerking toegezegd aan de ontwikkeling van een onderwijsagenda voor het HBO. Hierbij wordt de samenwerking gezocht met het (door OCW gefinancierde) Regieorgaan SIA en het Cybersafety Research and Education Network. Voor het MBO wordt aansluiting gezocht bij lopende initiatieven rond informaticaonderwijs en het Techniekpact. Ook is in 2014 de Cyber Security Academie opgericht, die een post-doctorale masteropleiding cybersecurity verzorg en die recent is gestart met 20 studenten. Het WODC heeft een onderzoek uitgezet naar de vraag naar diverse soorten werknemers die een rol spelen bij cybersecurity werknemers en het aanbod aan onderwijs waarlangs deze worden opgeleid en om/bijgeschoold. Dit onderzoek wordt begin 2015 opgeleverd.

Ontwikkelen van een cyber Defensie opleidings- en trainingstraject met private partijen en Regionale opleidingscentra (Actiepunt 34)

Samen met onderwijsinstellingen worden cyber Defensie opleidings- en trainingstrajecten ontwikkeld die aansluiten bij behoefte aan cyber-expertise binnen Defensie. Momenteel volgen 14 personen een opleiding bij een private partij. De eerste klas is in 2015 klaar.

Stimuleren van innovatie in cybersecurity (actiepunt 34, 36, 37)

Om innovatie in cybersecurity te stimuleren krijgt onderzoek een impuls en worden stappen gezet om een verbeterd inzicht te krijgen in de onderzoek behoefte van bedrijfsleven en maatschappij en het realiseren van een betere aansluiting tussen wetenschap en praktijk. Agentschap NL/RvO en NWO hebben, binnen de kaders van de in 2012 gelanceerde Nationale Cyber Security Research Agenda II (NCSRA II), een tweede tender voor de NCSRA in juni 2014 uitgeschreven ter waarde van ongeveer € 5,5 miljoen, ongeveer gelijk verdeeld over een SBIR programma voor korte termijn R&D en lange termijn onderzoek. In 2015 wordt een cybersecurity platform voor bedrijven, kennis- en (hoger)onderwijsinstellingen gelanceerd. Het inrichtingsplan voor dit cybersecurity research & education platform is gereed. In 2015 wordt door TNO en

NWO een plan opgesteld voor een verbeterd inzicht in de onderzoek behoeften van bedrijfsleven en maatschappij en het creëren van een sterkere verbinding en aansluiting tussen vragers en aanbieders met lopend en toekomstig onderzoek.